



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **07087564 A**(43) Date of publication of application: **31.03.95**

(51) Int. Cl. **H04Q 7/38**
H04L 9/32

(21) Application number: **05182185**(71) Applicant: **NEC CORP**(22) Date of filing: **29.06.93**(72) Inventor: **YAHAGI MASAHIKO**(54) **AUTHENTICATION SYSTEM**

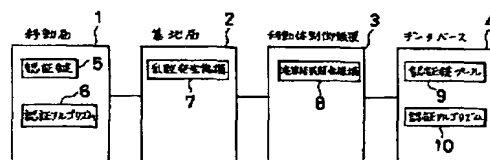
result and judges that the mobile station 1 is right when a collation result coincides.

(57) Abstract:

COPYRIGHT: (C)1995,JPO

PURPOSE: To perform an authentication without the necessity of a means preliminarily storing the authentication random number and the authentication arithmetic result corresponding to each mobile station and without retrieving the authentication key of a subscriber from a data base when a subscriber authentication is performed.

CONSTITUTION: At the time of the authentication of a mobile station 1, when the mobile station 1 receives an authentication request signal from a base station 2, the station 1 performs an authentication arithmetic execution and returns an authentication response to the base station 2. When a mobile object controller 3 receives an authentication confirmation signal, the controller transmits an authentication arithmetic result request to a data base 4. The data base 4 receiving it the authentication arithmetic execution, defines the obtained authentication arithmetic result as the set parameter of the response of the authentication arithmetic result and transmits the parameter to the mobile object controller 3. The mobile object controller 3 receives the response of the authentication arithmetic



(19)日本国特許庁 (J P)

(12) 特 許 公 報 (B 2)

(11)特許番号

第2531354号

(45)発行日 平成8年(1996)9月4日

(24)登録日 平成8年(1996)6月27日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所	
H 0 4 Q	7/38		H 0 4 B	7/26	1 0 9 S
H 0 4 L	9/32		H 0 4 L	9/00	A

請求項の数3(全10頁)

(21)出願番号	特願平5-182185	(73)特許権者	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22)出願日	平成5年(1993)6月29日	(72)発明者	矢萩 雅彦 東京都港区芝五丁目7番1号 日本電気 株式会社内
(65)公開番号	特開平7-87564	(74)代理人	弁理士 山川 政樹
(43)公開日	平成7年(1995)3月31日	審査官	清水 稔
		(56)参考文献	特開 平4-233341 (J P, A)

(54)【発明の名称】 認証方式

1

(57)【特許請求の範囲】

【請求項1】 認証に使用される認証鍵、基地局より送信される認証乱数と認証鍵を入力情報として認証演算を行う認証アルゴリズムを有する移動局と、
移動局および基地局以外の構成要素により発生させた乱数攪拌のための乱数の種に基づいて認証乱数を発生する機構、認証乱数とその認証乱数を移動局に送信し得られた認証演算結果と移動局識別番号を移動体制御装置に送出する手段を有する基地局と、
基地局より送信された移動局識別番号と認証乱数をデータベースに送信し得られた認証演算結果と基地局より送信された認証演算結果を照合する機構を有する移動体制御装置とを設け、
認証に使用する認証鍵、受信した認証乱数とその認証鍵を入力情報として認証演算を行う認証アルゴリズムと認

2

証演算結果を応答する機構を持つデータベースを構成要素とし基地局において認証が必要であると認識した時点で基地局で発生させた乱数を認証乱数として移動局に認証演算要求を行い、移動局より応答のあった認証演算結果を基地局において受信し、その認証乱数とその認証演算結果と移動局の識別番号を信号の設定パラメータとして移動体制御装置を基地局が起動し、
移動体制御装置において基地局より受信した信号の設定パラメータ内の認証検算結果を受信し、基地局より受信した信号の設定パラメータ内の認証演算結果とデータベースより応答のあった認証演算結果を照合し、この照合結果が一致した場合に認証確認がなされたと判断することを特徴とする認証方式。

【請求項2】 請求項1において、基地局は、移動体制御装置またはデータベースにて発生させた乱数の種に基

づいて認証乱数を発生することを特徴とする認証方式。

【請求項3】 請求項1において、移動局には1つ以上の認証対象があることを特徴とする認証方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、移動体通信システムの認証方式に関するものである。

【0002】

【従来の技術】従来の認証方式は図7に示すように移動局より親局（本発明の基地局と移動体制御装置を共に含む装置に対応）が発信要求を受け付けた時点で、親局はデータベース（本発明のデータベースに対応）に対し、識別番号（本発明の移動局識別番号に対応）を設定パラメータとして供給する。データベースは移動機認証情報を親局に返送するので、親局は移動局に対しコールプロック（CALL PROC）信号を返答後、親局で発生させた乱数を認証乱数として移動局に送出して認証要求（本発明では認証演算要求に対応）を行い、移動局より応答のあった認証応答に含まれる認証認証演算結果を得る。

【0003】親局はこの処理と別に移動局に送出した認証乱数を移動機認証情報により親局内で認証演算を行い、この認証演算結果と移動局より応答のあった認証応答に含まれる認証演算結果を照合し、この照合結果が一致した場合に認証確認がなされたと判断する。これは例えばPMT信号方式として、電子情報通信学会発行の信学技報（SSE92-75）に記載されている。

【0004】一方、図8および図9に示すように、複数の認証乱数とそれぞれの認証乱数に対応した複数の認証演算結果を前もって格納しておき、これを認証が必要ときに1組の認証乱数と認証演算結果として取り出し、移動局に対しその認証乱数を設定パラメータとして認証演算要求を行い、応答のあった認証演算結果と格納してあった認証演算結果を照合し、この照合結果が一致した場合に認証確認がなされたと判断する方式も規定されている。

【0005】これは文献（Security Related Network Function; Recommendation GSM 03.20 Version: 3.3.2 Date: January 1991）に記載されており、具体的には図8においてBS/MSC/VLRが移動局の認証関連情報を必要とするとき、BS/MSC/VLRはHLR/ACに対しリクエスト（Security Related Information Request）信号を送出する。

【0006】HLR/ACはその信号を受信すると目的とする移動局のKi（本発明の認証情報に対応）とHLR/AC内で発生した複数の乱数RAND（1、2、・・・n）を入力パラメータとし、認証アルゴリズムA3（本発明の認証アルゴリズムに対応）に使用し、複数の認証演算結果SRES（1、2、・・・n）を算出する。その後、HLR/AC内で発生した複数の認証乱

数と複数の認証演算結果はレスポンス（Authentication Vector Response）信号の設定パラメータとしてBS/MSC/VLRに伝送される。

【0007】BS/MSC/VLRは受信した複数の乱数と複数の認証演算結果を自己の記憶装置に格納する。その後、移動局（本発明の移動局に対応）の認証が必要となったときは図9に示す様な手順で認証動作を行う。すなわちBS/MSC/VLRは対象となる移動局の1組の認証乱数RAND（j）および認証演算結果SRES（j）を選択し、RAND（j）を設定パラメータとして移動局に対し認証要求（Authentication Request・本発明の認証演算要求）信号を送出する。この時、移動局は自己の有する認証鍵および認証乱数（RAND（j））を入力パラメータとして認証演算を行い、BS/MSC/VLRに返す。BS/MSC/VLRは予め選択したSRES（j）と移動局より応答のあった認証演算結果を照合し、この照合結果が一致した場合に認証確認がなされたと判断する。

【0008】

【発明が解決しようとする課題】しかしながらこのような前者の認証方法では親局からデータベースへの発信情報読出要求に対する応答として発信情報読出応答信号を返し、その発信情報読出信号の設定パラメータ内に移動機認証情報を含んでいるために、親局とデータベースとの間に張られた通信回線で送受される信号を第三者が傍受することあるいは、第三者がデータベースに対して情報読出要求を送出することによって移動局番号（IMSI）と対応する移動機認証情報を第三者が知ることができる恐れがあった。

【0009】また後者の認証方法ではBS/MSC/VLR内にBS/MSC/VLRの関与する移動局毎に複数の認証乱数と対応する複数の認証演算結果を蓄積する記憶機能を有しなければならないという問題があった。

【0010】本発明はこのような従来の課題を解決するためになされたもので、個々の移動局に対応した認証乱数と認証演算結果をあらかじめ格納する手段を必要とせず、かつ加入者認証の際、加入者の認証鍵をデータベースから引き出すことなく認証を行うようにしたものである。

【0011】

【課題を解決するための手段】このような課題を解決するために本発明による認証方式は、移動局および基地局以外の構成要素により発生させた乱数攪拌のための乱数の種に基づいて認証乱数を発生して移動局に認証要求を行い、移動局より送られる認証応答に含まれる認証演算結果と、認証乱数と移動局識別番号を移動体制御装置に送出する基地局と、基地局より送信された移動局識別番号と認証乱数をデータベースに送信し得られた認証演算結果と基地局より送信された認証演算結果を照合する移動体制御装置と、認証に使用する認証鍵、受信した認証

乱数とその認証鍵とを入力として認証演算を行い、認証結果を出力するデータベースとを備えている。

【0012】

【作用】移動局および基地局以外の構成要素により発生させた乱数攪拌のための乱数の種に基づいて基地局において認証乱数を発生し、移動局に対し認証要求を行い、認証乱数と認証対象識別番号と移動局より送られる認証10 応答に含まれる認証演算結果を移動局制御装置に送出し、移動体制御装置は受信した認証対象識別番号と、乱数をデータベースに送信し、得られた認証演算結果と基地局より受信した認証演算結果を照合することによって認証を行う。

【0013】

【実施例】図1は本発明の一実施例の各構成要素が有する情報および機構を示す構成図である。移動局1は通常送信を行うことを意図するユーザによって所有され自己の装置内に認証鍵5および基地局2より送られる認証乱数と認証鍵5を入力パラメータとして認証演算を行う認証10 アルゴリズム6を有する。基地局2は自己の装置内に移動局1に対して認証要求を行う際、送出するに認証乱数を自律的に発生する乱数発生機構7を有する。移動体制御装置3は自己の装置内に移動局1より応答のあった認証演算結果と移動局1に対し送出した認証乱数と同一の乱数を認証乱数としてデータベース4に認証演算要求を送出することにより、得られた認証演算結果を照合する機能を持つ演算結果照合機構8を有する。

【0014】データベース4は自己の装置内に移動局毎に異なり得る複数の移動局の認証鍵プール9と、移動体制御装置3より送られる認証乱数および同時に移動体制御装置3より送られる移動体識別番号により認証鍵プール9より得られる特定の移動局の認証鍵を入力パラメータとして認証演算を行う認証アルゴリズム10を有する。図2は各構成要素間で転送される情報を図示したものである。基地局12は移動局11の認証が必要と判断した時点で自己の装置内にある乱数発生機構17より自律的に乱数を発生する。その後、基地局12は発生した乱数を認証乱数として、この認証乱数を設定パラメータとした移動局への認証演算要求信号21を移動局11に送出する。

【0015】移動局11は基地局12より受信した移動局への認証演算要求信号21内に含まれる認証乱数と自己の装置内に記憶している認証鍵15を入力パラメータとして、自己の装置内にある認証アルゴリズム16を使用して、認証演算を行う。その後、移動局11は認証アルゴリズム16によって得られた認証演算結果を設定パラメータとし、移動局からの認証応答信号22を基地局12に送出する。基地局12は移動局からの認証応答信号22を受信すると、自己の装置内で発生した乱数と移動局からの認証応答信号22に含まれる認証演算結果と、移動局11を示す移動局識別番号を設定パラメータ

とした基地局から移動体制御装置への認証確認信号23を移動局制御装置13へ送出する。

【0016】移動体制御装置13は基地局から移動体制御装置への認証確認番号23を受信すると、その信号内に含まれる移動局識別番号と乱数を設定パラメータとした移動体制御装置からデータベースへの認証演算要求信号24をデータベース14に送出する。データベース14は移動体制御装置からデータベースへの認証演算要求信号24を受信すると、その信号内に含まれる移動局識別番号を入力パラメータとし、認証鍵プール19をアクセスし、移動局識別番号に関連する認証鍵を得、その認証鍵と移動体制御装置13からデータベース14への認証演算要求信号24に含まれる乱数を入力パラメータとし、自己の装置内にある認証アルゴリズム20を使用して認証演算を行う。

【0017】その後、データベース14は認証アルゴリズム20によって得られた認証演算結果を設定パラメータとし、データベース14から移動体制御装置13へ認証演算結果応答信号25を送出する。移動体制御装置13はデータベース14から認証演算結果応答信号25を受信すると、その信号内に含まれる認証演算結果を基地局12から以前受信した移動局11に関する認証演算結果要求信号23に含まれる認証演算結果を自己の装置内に含まれる演算結果照合機構18によって照合し、この照合結果が一致した場合に移動局が正当であると判断する。

【0018】図3は移動局、基地局、移動体制御装置、およびデータベース間の信号転送タイミングと、個々の信号に含まれる主要パラメータを図示したシーケンス図である。移動局の認証が必要となったとき、基地局は乱数発生30を行い、ここで発生した乱数を限定パラメータとし、移動局に認証要求信号31を送出すると、移動局はパラメータに含まれる乱数を使用して、認証演算実行32を行う。その後、移動局が認証演算実行32によって得られた認証演算結果を設定パラメータとし、基地局に認証応答33を送出すると、基地局は認証応答信号のパラメータに含まれる認証演算結果、基地局で発生した乱数および移動局識別番号を設定パラメータとし、認証確認信号34を移動体制御装置に送出する。

【0019】移動体制御装置は基地局から認証確認要求を受信すると、データベースに対してそのパラメータに含まれる乱数と、移動局識別番号を設定パラメータとし、認証演算結果要求35を送出する。データベースは移動体制御装置から認証演算要求35を受信すると、そのパラメータに含まれる移動局識別番号より特定の移動局に対応する認証鍵を求め、その認証鍵と認証演算要求のパラメータに含まれる乱数を用いて認証演算実行36を行い、得られた認証演算結果を認証演算結果応答37の設定パラメータとし、移動体制御装置に送出する。移動体制御装置は認証演算結果応答37を受信すると、そ

のパラメータに含まれる認証演算結果と、認証確認要求34に含まれる認証演算結果を照合し、照合結果が一致した場合に移動局が正当であると判断する。

【0020】図1、図2、図3によって説明した認証方法を用いることにより、従来の認証方法では移動体制御装置とデータベース間に張られた通信回線で送受される信号を第三者が傍受することあるいは、第三者がデータベースに対して情報読み取り要求を送出することによって第三者が移動局識別番号に対応する認証番号を知られる恐れがあったが、この恐れを減少させることができるという効果がある。即ち、移動体制御装置とデータベースとの間に張られた通信回線で送受される信号を傍受しても知ることができる情報はある移動局に対して認証要求を行った場合の一時的な認証乱数と対応する認証演算結果の組み合わせのみであり、この組み合わせから実際の移動局に対応する認証鍵を推測することは移動局と基地局の間の通信回線を傍受する場合と同等の困難性を有する。

【0021】また、データベース自身が公衆回線から情報読み取り要求に対応する応答機能を持たず、データベースに直接接続されている入力装置あるいは専用線によって接続されている特定の入力装置以外に情報読み取り要求を受け付けなくする構成にすることにより、第三者が移動局識別番号に対応する認証鍵を知る可能性を減少させることができる。また、この認証方式は移動体通信システムが複数の事業者によって構築された場合、移動局識別番号に対応する認証鍵が事業者間で転送されなくなる。一方、従来の認証方法では移動局の認証乱数と対応する認証演算結果を認証鍵を保持するデータベース以外の装置に蓄積する必要があり、付加的な記憶装置を必要としたが、この記憶装置を必要としない効果もある。

【0022】図4および図5は請求項2に関連する基地局で発生する乱数の発生方法を示すシーケンス図である。図4において、移動体制御装置は乱数発生40を行い、乱数種を設定パラメータとした乱数初期化要求41を基地局に送出する。基地局は乱数初期化要求41を受信すると、パラメータに含まれる乱数種発生を基地局内に含まれる乱数発生機構に入力し、乱数初期化42を行い、基地局で発生する乱数の初期化を行う。また、図5においてデータベースは乱数種発生50を行い、乱数種設定パラメータとした乱数初期化要求51を移動体制御装置に送出し、移動体制御装置は乱数初期化要求51を受信すると、パラメータに含まれる乱数種を基地局に含まれる乱数種発生機構に入力し、乱数初期化53を行い、基地局で発生する乱数の初期化を行う。

【0023】図4、図5によって説明した認証方法を用いることにより、基地局で発生する乱数の値が繰り返される現象等が発生し、この現象を回避する必要性が生じたとき、基地局以外の構成要素の作用によって、乱数の値を変更可能となる効果がある。図6は請求項3に関連

し、移動局に2つの認証対象がある場合に各構成要素間で転送される情報の一例を示すものである。基地局63は2つの認証対象、即ち認証対象62を有する移動局の認証が必要であると判断した時点で自己の装置内にある認証対象61のための乱数発生機構71および認証対象62のための乱数発生機構72により自律的に乱数A、乱数Bを発生する。

【0024】その後、基地局63は発生した乱数A、乱数Bをそれぞれ認証対象61、認証対象62への認証演算要求75の認定パラメータとし、移動局へ認証演算要求75を送出する。移動局は受信した認証演算要求75の設定パラメータに含まれる乱数A、Bをそれぞれ認証対象61、62に分配し、認証対象61は認証鍵67と、認証アルゴリズム68と、乱数A、認証対象62は認証鍵69と、認証アルゴリズム70と、乱数Bを使用してそれぞれ独立に認証演算結果A、認証演算結果Bを算出して、その結果を認証演算応答結果78として送出する。基地局63は認証演算結果応答78を受信すると、認証確認要求79の設定パラメータとして、認証演算結果A、乱数A、認証対象61、識別番号、認証演算結果B、乱数B、識別番号を改訂し、認証確認要求79を移動体制御装置64へ送出する。

【0025】移動体制御装置64は認証確認要求79を受信すると認証確認要求79の設定パラメータに含まれる認証対象61の識別番号と、乱数Aを認証演算要求80の改訂パラメータ、認証対象62、識別番号と乱数Bを認証演算要求82の設定パラメータとし、認証対象61、データベース65と認証対象62、データベース66に対しそれぞれ認証演算要求80、認証演算要求82を送出する。認証対象61、データベース65、認証対象62、データベース66は認証演算要求80、認証演算要求82をそれぞれ受信すると、それぞれの設定パラメータに含まれる情報を用いて独立に認証演算を行い、認証演算結果を認証演算結果応答81、認証演算結果応答83の設定パラメータとし、移動体制御装置64に認証演算結果応答83を送出する。

【0026】移動体制御装置64は認証対象61、データベース65から認証演算結果応答81を受信すると、その設定パラメータに含まれる認証演算結果と、基地局63から受信した認証確認要求79に含まれる認証演算結果Aを照合し、認証対象61の認証を行う。同様に、認証対象62、データベース66から認証演算結果応答83を受信すると、その設定パラメータに含まれる認証演算結果と基地局63から受信した認証確認要求79に含まれる認証演算結果Bを照合し、認証対象62Bの認証を行う。図6によって説明した認証方法を用いることにより、移動局が複数の認証対象を有し、それぞれの認証が必要な場合、たとえば移動局の端末装置の認証と移動局を使用するユーザの認証が必要な場合においても、同様の手順で認証が行える効果があり、図1、図2、図

3の認証方法と同等の効果得られる。

【0027】

【発明の効果】以上説明したように本発明は、基地局において認証乱数を発生し、移動局に対し認証要求を行い、認証乱数と認証対象識別番号と移動局より送られる認証応答に含まれる認証演算結果を移動局制御装置に送出し、移動体制御装置は受信した認証対象識別番号と、乱数をデータベースに送信し、得られた認証演算結果と基地局より受信した認証演算結果を照合することによって認証を行うようにしたので、データベースに含まれる認証対象の認証情報あるいは認証鍵が移動体制御装置とデータベースの間に張られた通信路内に現れず、その通信路内で送受される信号を傍受することによって認証対象の認証情報あるいは認証鍵を取得することを困難にするという効果を有し、認証対象に関連する複数の認証乱数と対応する複数の認証演算結果を複数の認証対象にわたり記憶する機構を必要としないという効果を有する。

【図面の簡単な説明】

【図1】各構成要素が有する情報及び機構を示す図である。

【図2】各構成要素間で転送される情報を示す図である。

【図3】各構成要素間の信号シーケンスを示す図である。

【図4】移動体制御装置が起動する基地局発生乱数の初期シーケンスを示す図である。

【図5】データベースが起動する基地局発生乱数の初期

化シーケンスを示す図である。

【図6】認証対象が2つある場合に各構成要素間で転送される情報を示す図である。

【図7】従来用いられている発信時の認証手順を示す図である。

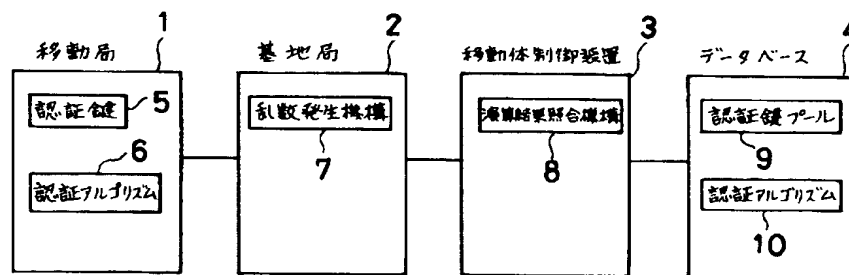
【図8】従来用いられている認証乱数および認証演算結果の格納方式を示す図である。

【図9】従来の認証手順を示す図である。

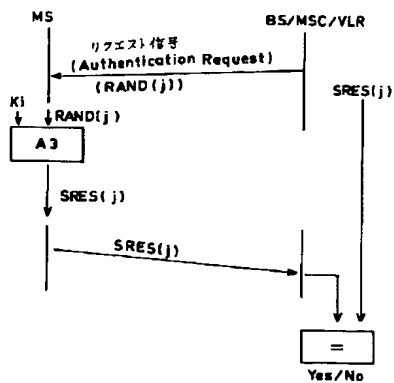
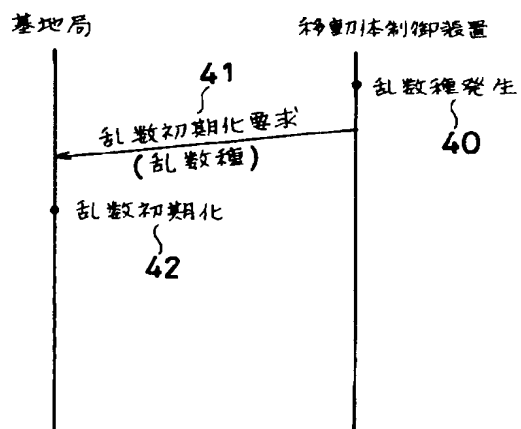
【符号の説明】

- 10 1、11 移動局
- 2、12 基地局
- 3、13 移動局制御装置
- 4、14 データベース
- 5、15 移動局内認証鍵
- 6、16 移動局内認証アルゴリズム
- 7、17 乱数発生機構
- 8、18 演算結果照合機構
- 10、20 データベース内認証アルゴリズム
- 21 移動局への認証演算要求信号
- 22 移動局からの認証応答信号
- 23 基地局から移動体制御装置への認証確認要求信号
- 24 移動体制御装置からデータベースへの認証演算要求信号
- 25 データベースから移動体制御装置への認証結果応答信号
- 75、76、80、82 認証演算要求
- 77、78、81、83 認証演算結果応答

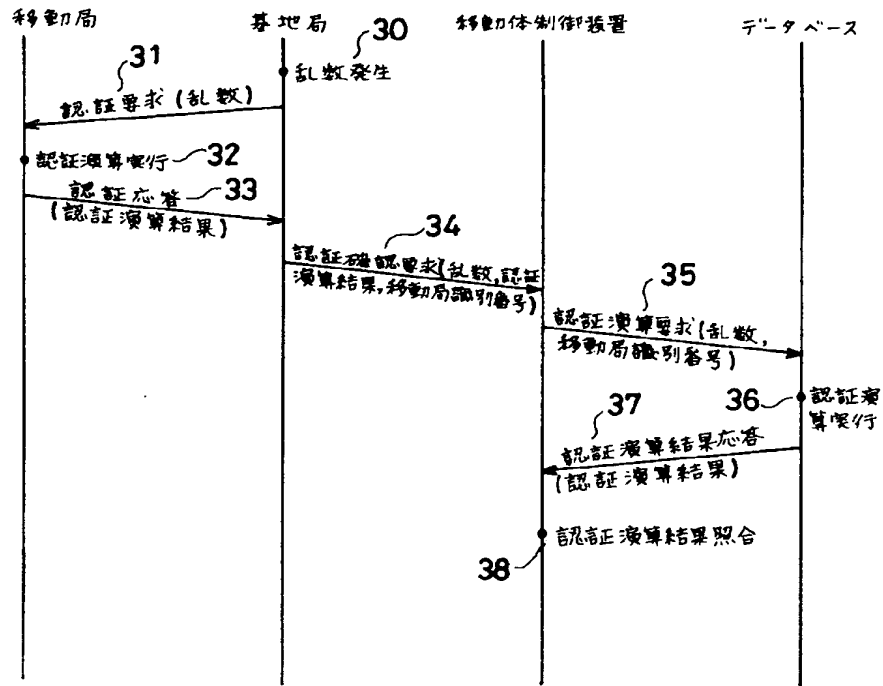
【図1】



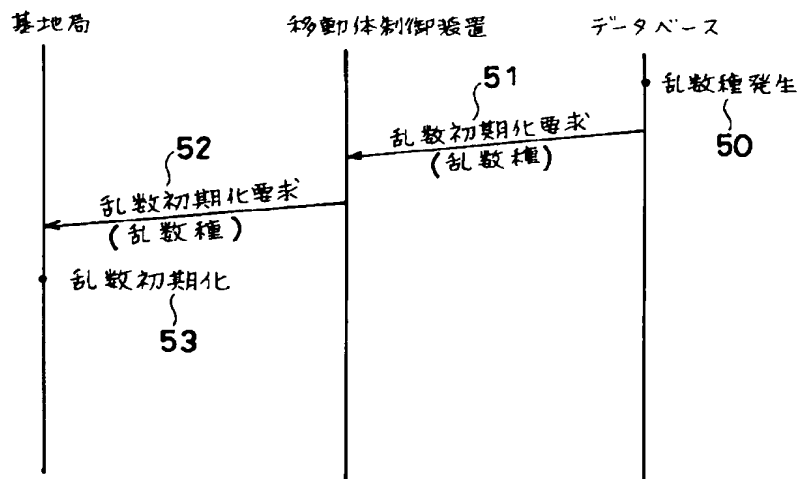
【图9】



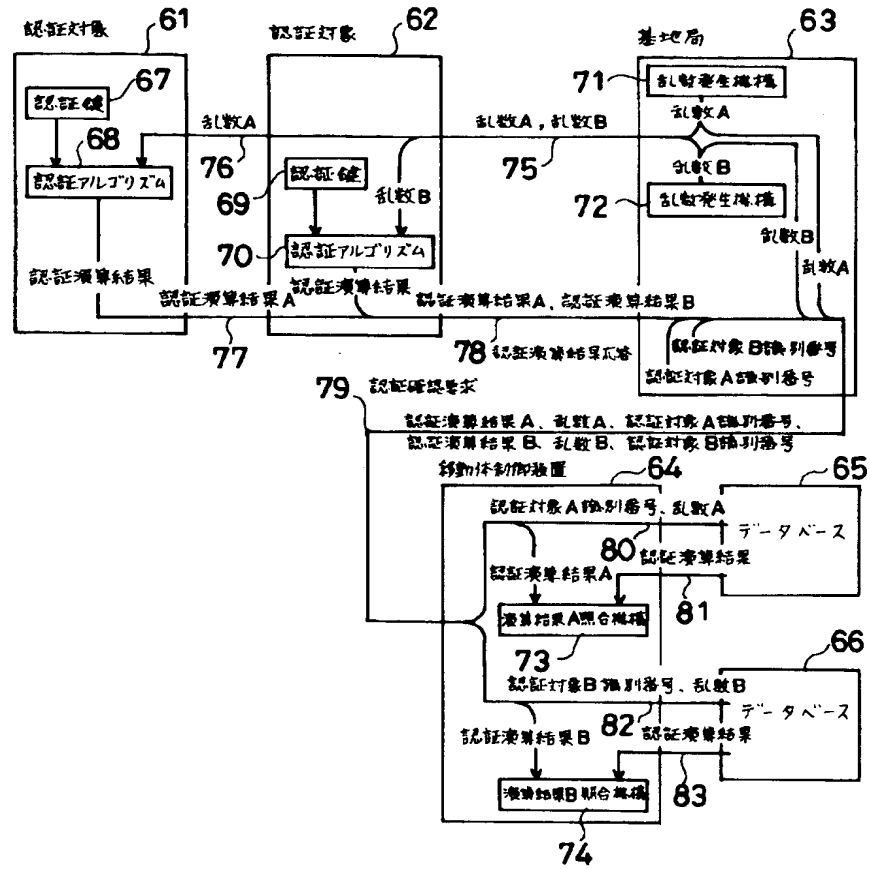
【図3】



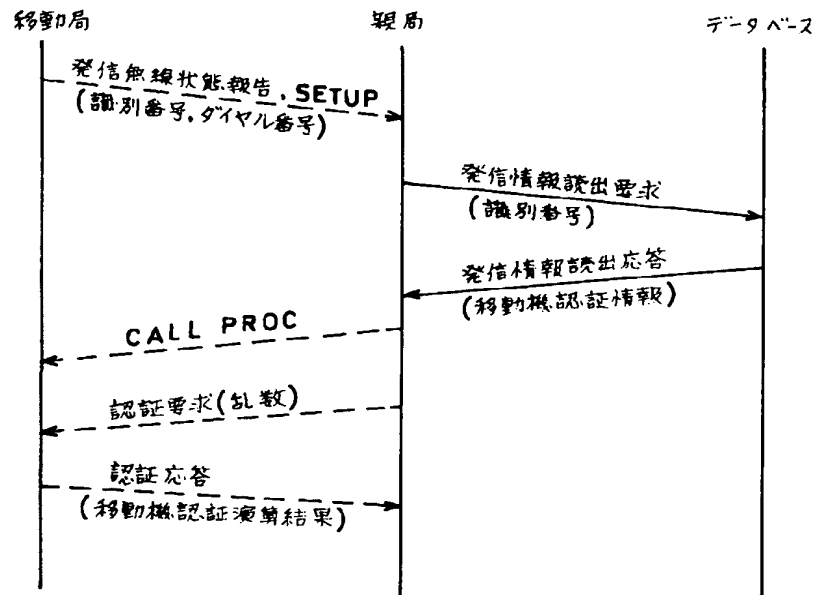
【図5】



【図6】



【図7】



【図8】

